UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

DOUGLAS BISHOP, individually and on behalf of all others similarly situated,
% DannLaw
15000 Madison Avenue
Lakewood, OH 44107

AND

CHARLES METZGER, individually and on behalf of all others similarly situated,
% DannLaw
15000 Madison Avenue
Lakewood, OH 44107

Plaintiffs

v.

BON SECOURS MERCY HEALTH, INC.
% Corporation Service Company, Registered Agent
3366 Riverside Drive, Suite 103
Upper Arlington, OH 43221

AND

PERRY JOHNSON & ASSOCIATES, INC.
% CT Corporation System, Registered Agent
701 S. Carson Street, Suite 200
Carson City, NV 87901

Defendant(s).

Case No.

Judge

COMPLAINT FOR DAMAGES

JURY DEMAND ENDORSED HEREON

Plaintiffs Douglas Bishop and Charles Metzger (collectively, the "Plaintiffs") bring this action individually, and on behalf of all others similarly situated, by and through counsel, against Defendants Bon Secours Mercy Health, Inc. d/b/a Mercy Health ("Mercy Health"), and Perry Johnson & Associates, Inc. ("PJ&A") (collectively, "Defendants") for damages and equitable

relief, including restitution, disgorgement, and injunctive relief for Defendants' violations of the law that resulted in a data breach ("Data Breach") that allowed cybercriminals to steal the sensitive and confidential medical transcription records of nearly 9 million people.

INTRODUCTION

1. On or before March 27, 2023, Plaintiffs' and Class members' personal information contained in medical transcription records was accessed and stolen from Defendants' network servers in the Data Breach. The information that was accessed includes some of the most highly personal health and treatment information, such as name, date of birth, address, gender, medical record number, account number, Social Security numbers, insurance information, medical transcription files containing laboratory and diagnostic testing results, medications, treatment facilities, name of healthcare providers, admit diagnosis, and dates and times of service (the "protected health information," or "PHI").

2. On or before May 2, 2023, PJ&A was made aware that an unauthorized third party gained access to its computer network servers and absconded with computer files containing the PHI pertaining to millions of patients treated by hospitals and healthcare providers throughout the United States, including Mercy Health.

3. Defendants failed to comply with regulatory, ethical, and industry standards for cybersecurity and confidentiality of patient records, failed to take the most basic security measures such as encryption of data, destruction of obsolete data, employee training to prevent phishing attacks, and robust password requirements, and failed to prevent, detect, and adequately respond to a foreseeable data breach carried out by cyber criminals. As a result, criminals gained access to, copied, and stole Plaintiffs' and Class members' PHI.

4. Defendants' insufficient data security practices failed to prevent or detect the Data

Breach until it was too late. The criminals gained access to Defendants' computer networks, and remained there undetected from at least March 27, 2023 to May 2, 2023.

5. PJ&A unreasonably delayed providing notice to anyone regarding the Data Breach. PJ&A waited more than two months to alert Mercy Health. According to PJ&A, Mercy Health was made aware of the Data Breach on July 21, 2023.

6. The notice to impacted patients was even more unreasonably delayed. According to the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights Breach Portal (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last visited December 11, 2023), on November 3, 2023, PJ&A reported a hacking/IT incident impacting 8,952,212 individuals across the country. The notice letters to Plaintiffs were dated November 8, 2023.

7. Although PJ&A was made aware of the incident on May 2, 2023, and sent caution to Mercy Health on July 21, 2023, neither PJ&A nor Mercy Health notified Plaintiffs and Class members until November 8, 2023.

8. In all, Defendants allowed more than six (6) months (*i.e.,* May 2, 2023 to November 8, 2023) to lapse before sending notice to Plaintiffs and Class members from the date they first allegedly learned of the Data Breach, and over seven (7) months since the Data Breach first allegedly occurred.

9. As a direct result of the Data Breach, Plaintiffs and Class members have suffered numerous actual and concrete injuries and will suffer additional injuries into the future. Plaintiffs seek damages and other legal and equitable relief for the following categories of harms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) financial costs incurred due to actual identity theft; (e) the cost of future identity theft monitoring;

(f) loss of time incurred due to actual identity theft; (g) failure to receive the benefit of the bargain when Defendants failed to provide adequate and reasonable protection that caused the Data Breach; (h) deprivation of value of their PHI; (i) significant risk and degradation of the ability for their healthcare providers to provide adequate continuity of care; and (j) potential harm that disclosure of their PHI may limit future employment opportunities.

10. Plaintiffs and Class members seek redress for Defendants' unlawful conduct, including damages, restitution, and injunctive relief for Defendants' negligence, negligence *per se*, breach of implied contract, unjust enrichment, and Defendants' violation of Plaintiffs' and Class members' statutory rights to reasonable data security practices and reasonably timely notice of the Data Breach.

THE PARTIES

11. Plaintiff Douglas Bishop is a natural person and a citizen of Ohio.

12. Plaintiff Charles Metzger is a natural person and a citizen of Ohio.

13. PJ&A has its principal place of business in Nevada and is incorporated in Nevada. It is a business associate under HIPAA that provides medical transcription services for numerous health care providers, including Mercy Health.

14. Mercy Health has its principal place of business in Cincinnati, Ohio and is incorporated in Maryland. Mercy Health provides healthcare services to its patients.

JURISDICTION & VENUE

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because there are 100 or more members of the proposed class, at least one Class member (Plaintiffs) has diverse citizenship from at least one Defendant (PJ&A), and the amount in controversy exceeds $5,000,000, exclusive of costs.

16. The Court has personal jurisdiction over PJ&A because PJ&A transacts business in this state and enters into and performs contracts within this state, which are related to the claims asserted in this case.

17. The Court has personal jurisdiction over Mercy Health because the case arises out of the conduct of its agent (PJ&A) that occurred substantially within this state. Mercy Health transacts business in this state and enters into and performs contracts within this state, which are related to the claims asserted in this case.

18. Venue is proper under 28 U.S.C. § 1391 because each of the Defendants are subject to personal jurisdiction in this district with respect to this action.

FACTUAL ALLEGATIONS

Defendants' Promises and Obligations Regarding Protection of PHI

19. Mercy Health provides healthcare services to patients. Mercy Health contracted with PJ&A to perform medical transcription services as appropriate in facilitating Mercy Healths' care of its patients, including Plaintiffs and Class members. In addition to Mercy Health, many other healthcare providers contracted with PJ&A to perform medical transcription services in providing care for their patients, including Class members.

20. Plaintiffs and Class members obtained treatment from healthcare providers that used PJ&A and were required to provide Defendants with considerable information including but not limited to: name, date of birth, address, gender, medical record number, account number, Social Security number, insurance information, medical transcription files containing laboratory and diagnostic testing results, medications, treatment facilities, name of healthcare providers, admit diagnosis, and dates and times of service ("PHI").

21. Plaintiffs and Class members relied on Defendants, who are licensed medical treatment providers, to maintain the integrity of their PHI, to keep their PHI confidential and secure, to use it only for purposes of treatment and billing for authorized treatment, and to implement and follow adequate and reasonable data collection, storage, and retention policies. Defendants transmitted, maintained, and stored the PHI on systems and networks that were inadequately protected and ultimately accessed without authorization by criminals in the Data Breach.

22. Defendants owed Plaintiffs and Class members numerous statutory, regulatory, ethical, contractual, and common law duties to safeguard and keep Plaintiffs' and Class members' PHI confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, and theft.

23. In its notice of privacy practices, Mercy Health promises to Plaintiffs and Class members that Mercy Health is "committed to protecting medical information about you" and is "required by law to make sure that your medical information is protected." Mercy Health promises to use PHI only for treatment, healthcare operations, and payment. *See* Exhibit 1 - Notice of Privacy Practices

24. Contrary to these promises and its ethical and professional obligations, Mercy Health shared with PJ&A the PHI of Plaintiffs and Class members without adequate oversight, due diligence, and assurances that PJ&A would keep the PHI safe and secure and, as a result of Defendants' failures, the Data Breach occurred.

The Data Breach

25. On or before March 27, 2023, an unauthorized third party gained access to PJ&A's network servers. The notice letter sent to Plaintiffs does not state who informed PJ&A, or how

PJ&A learned about the Data Breach. The letter does not include details regarding the length of the Data Breach. According to the HHS breach portal on December 11, 2023, the Data Breach was a "Hacking/IT incident" impacting one or more "Network Servers" and resulted in the theft of PHI concerning 8,952,212 patients.

26. Based on Defendants' concession that the unauthorized access occurred between at least March 27, 2023 and May 2, 2023, it is reasonable to conclude that the criminals were able to gain access undetected and unimpeded for long enough to satisfy themselves that they had extracted all sensitive and valuable information from PJ&A's networks.

27. On approximately May 2, 2023, PJ&A became aware of the Data Breach and began to take measures to hire a cybersecurity vendor to "assist with the investigation, contain the threat, and further secure our systems."

28. On July 21, 2023, PJ&A alerted its healthcare provider clients of the Data Breach, including Mercy Health.

29. Plaintiff Bishop received his letter notifying him of the Data Breach after November 8, 2023. *See* Exhibit 2**.**

30. Plaintiff Metzger received his letter notifying him of the Data Breach on November 28, 2023. See Exhibit 3.

31. The letter attempts to downplay the severity of the situation by claiming without any substantiation that "we are not aware of any instances of fraud or identity theft involving your personal information…" *Id.* Nevertheless, Defendants advise Plaintiffs and Class members to take steps to "review any statements you receive from your healthcare providers," and to "remain vigilant by reviewing account statements and monitoring credit reports." *Id.*

32. Currently, the full extent of the types of sensitive personal information, the scope of the Data Breach, and the details regarding how the Data Breach was carried out are all within the exclusive control of Defendants and their agents, counsel, and forensic security vendors. However, Plaintiffs and Class members are aware that the stolen PHI provides a one-stop shop for identity thieves to wreak complete havoc on their lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, medical conditions, diagnoses, treatment information, and dates of birth), and the criminal targeting, theft and publication of the data on the internet, Plaintiffs and Class members have all experienced a materialized and imminent risk of identity theft.

33. The PHI that was exfiltrated in the Data Breach was held in unencrypted form by Defendants, and included Plaintiffs' and Class members' PHI.

The Data Breach Was Preventable

34. Defendants could have prevented the Data Breach by properly securing and encrypting the PHI of Plaintiffs and Class members, by properly training their employees and contractors to recognize and prevent cybersecurity risks, and/or by implementing and following adequate procedures to monitor and detect data breaches. Defendants' negligence in safeguarding the PHI of Plaintiffs and Class members was exacerbated by the repeated warnings and alerts directed to U.S. companies warning that they should protect and secure sensitive data, especially in light of the substantial increase in cyberattacks specifically targeting healthcare providers.

The Data Breach Was Foreseeable

35. The FBI has been warning healthcare providers, such as Defendants, about the threat posed by the ransomware and others, and to be on the lookout for attacks.

36. The United States Cybersecurity & Infrastructure Security Agency, Department of Justice, and Department of Health & Human Services issued a Joint Cybersecurity Advisory as early as on October 28, 2020, warning of an acute threat to U.S. hospitals and healthcare providers and advising them on how to "ensure that they take timely and reasonable precautions to protect their networks from these threats."[1] The Advisory details at great length the pathways of specific viruses, malware, and online threats, and lists numerous mitigation steps, including:

a) Patch operating systems, software, and firmware as soon as manufacturers release updates;

b) Check configurations for every operating system version for organization-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled;

c) Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts;

d) Use multi-factor authentication where possible;

e) Disable unused remote access/remote desktop protocol (RDP) ports and monitor remote access/RDP logs;

f) Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy;

g) Audit user accounts with administrative privileges and configure access controls with least privilege in mind;

[1] https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited November 16, 2023).

h) Audit logs to ensure new accounts are legitimate;

i) Scan for open or listening ports and mediate those that are not needed;

j) Identify critical assets such as potential database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network;

k) Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment;

l) Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

37. In addition, the Advisory emphasizes a focus on awareness and training. Because end users are targeted, employees need to be aware of threats and how they are delivered.

38. On information and belief, the hackers who carried out the Data Breach used rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails. Such attacks are entirely preventable through proper training of employees to recognize phishing emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

39. Even with a successful initial infection vector through basic phishing techniques, the Data Breach could have been identified and halted quickly had Defendants implemented widely available software capable of fully detecting and preventing the Data Breach.

40. Despite the well-known risks and availability of reasonable and effective protections, Defendants inexplicably failed to properly train employees and vendors, failed to exercise appropriate oversight and quality assurance, failed to implement industry standard

security measures, and maintained highly sensitive patient information in a manner they knew or should have known was vulnerable to access and exfiltration.

41. Despite the prevalence of public announcements of these data breach and data security compromises and despite numerous attempts on the part of the federal government to inform Defendants about the threats facing them and ways to prevent attacks, and despite having ample time to implement precautions and training, Defendants were negligent and did not adequately prepare for this wholly foreseeable event; thus, allowing extremely sensitive data to be accessed, viewed, and stolen by the criminals. Defendants breached their duties to take appropriate steps to protect Plaintiffs' and Class members' PHI from being compromised and failed to adequately notify them that the Data Breach took place.

42. Unfortunately for Plaintiffs and Class members, their PHI was not secured in the manner required by law that would have prevented the Data Breach.

43. What is worse, despite Defendants' obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendants failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, and failed to include in the Data Breach notification letter a sufficient description of the Data Breach or the information needed by Plaintiffs and Class members to react appropriately to the Data Breach, including taking whatever mitigation measures are necessary.

44. Defendants had specific obligations imposed on them by contracts and law to ensure the adequate protection of Plaintiffs' and Class members' PHI as covered entities and business associates under HIPAA.

Defendants' HIPAA Violations

45. Defendants are regulated by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), and are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendants' protection of medical information maintained in electronic form.

46. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

47. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

48. HIPAA's Security Rule requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by its workforce.

49. HIPAA also requires Defendants to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement

technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

50. The facts of the Data Breach establish that Defendants failed to comply with these Rules. The Data Breach resulted from a combination of inadequacies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by their workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and,

(j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

Defendants Violated Federal Trade Commission Guidelines

51. Defendants also violated the duties applicable to them under the Federal Trade Commission Act (15 U.S.C. § 45, *et seq*.) from engaging in "unfair or deceptive acts or practices

in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

52. As established by these laws, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the medical information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiffs and Class members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that their computer systems, networks, and protocols adequately protected this medical information and were not exposed to infiltration. This also included a duty to Plaintiffs and Class members to design, maintain, and test their computer systems to ensure that the PHI was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the PHI through processes such as phishing, including adequately training employees and others who accessed information within their systems on how to adequately protect this information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of their data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI from theft; and to disclose in a timely and accurate manner when data breaches occurred.

53. Defendants also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems. It is apparent that Defendants did not do so.

54. Defendants owed these duties to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in criminals successfully carrying out a cyberattack and exfiltrating Plaintiffs' and Class members' PHI, to the injury and detriment of Plaintiffs and Class members. By taking affirmative acts inconsistent with these obligations that left Defendants' computer systems foreseeably vulnerable to criminals, Defendants disclosed and/or permitted the disclosure of PHI to unauthorized third parties. Defendants thus failed to preserve the confidentiality of PHI they were duty-bound to protect. Instead, Defendants became the centralized, data-rich location where a criminal could reap exponential profits in one cyberattack, rather than 9 million individual attacks to Plaintiffs and Class members individually.

Defendants' Conduct Violates Ohio Standards for Healthcare Duty of Confidentiality and Authorization for Disclosure of Medical Information

55. Under Ohio law, a health care provider may not disclose personally identifiable non-public information about a patient without the patient's express written authorization.

56. Ohio Rev. Code § 3798.04 provides that a covered entity, such as a health care provider, shall not "use or disclose protected health information without any authorization that is valid under 45 C.F.R. 164.508, and if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R. part 2."

57. The Ohio Supreme Court has recognized that persons in possession of PHI owe a duty of confidentiality and that "an independent tort exists for the unauthorized, unprivileged disclosure to a third-party of nonpublic medical information that a physician or hospital has

learned with a patient-physician relationship." *Biddle v. Warren Gen. Hosp*., 68 Ohio St. 3d 395, 401 (1999).

58. Confidentiality is a cardinal rule of the provider-patient relationship.

59. Plaintiffs were aware of Defendants' duty of confidentiality, and as a result, have objectively reasonable expectations that Defendants will not share or disclose, whether intentionally or unintentionally, their private information in the absence of authorization for any purpose that is not directly related to or beneficial to patient care.

Value of Personally Identifiable Information

60. PHI has significant value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[2] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[3] Criminals can also purchase access to entire company data breaches for $900 to $4,500.

61. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your

[2] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 11, 2023).

[3] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed December 11, 2023).

> number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[4]

62. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

63. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[5]

64. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

65. A robust cyber black market exists in which criminals post stolen medical information on multiple dark web sites to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. According to a 2017 Javelin

[4] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 11, 2023).

[5] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed December 11, 2023).

strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and six years old had increased by nearly 400% over the previous four years.[6]

66. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[7] PHI can be sold at a price ranging from approximately $20 to $300.[8]

67. In this case, all evidence indicates that Plaintiffs' and Class members' PHI was left unprotected, to be exfiltrated by criminals and sold on the dark web. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by anyone with an Internet connection.

68. Medical identity theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences if a victim's health information is mixed with other records. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[9]

---

[6] *See,* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed December 11, 2023).

[7] *Id.*

[8] https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 11, 2023).

[9] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-theft/ (last accessed Nov. 16, 2023); See also, Medical Identity Theft in the New Age of Virtual Healthcare, IDX (March 15, 2021), https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed December 11, 2023).

69. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[10]

70. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[11]

71. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security numbers and names, is impossible to "close" and difficult, if not impossible, to change.

72. These data demand a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

73. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

---

[10] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessedDecember 11, 2023).

[11] Ponemon Institute, Fifth Annual Study on Medical Identity Theft, (February, 2015), http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last accessedDecember 11, 2023).

[12] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 11, 2023).

74. The fraudulent activity resulting from the Data Breach may not come to light for years.

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

76. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PHI of Plaintiffs and Class members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

77. Plaintiffs and Class members now face years of constant surveillance of their financial, medical, and personal records and bills, credit and financial account monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PHI.

78. Defendants were, or should have been, fully aware of the unique type and the significant volume of unencrypted and unsegmented data on Defendants' network servers and database servers, amounting to millions of individuals' detailed PHI.

---

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao. gov /assets/gao-07-737.pdf (last accessed December 11, 2023).

79. Defendants have not prevented the criminals from disclosing Plaintiffs' and Class members' PHI on the Internet. Defendants have not retrieved and cannot retrieve the PHI. Thus, the PHI remains in circulation on the Internet for access, viewing, and misuse, causing damage to Plaintiffs and Class members and breaching their confidentiality.

80. Defendants have not provided sufficient information in their untimely Data Breach notice letters such that Plaintiffs and Class members could understand and appreciate the full nature of the risk to them caused by Defendants' Data Breach, allowing them to make informed decisions about how to protect themselves and their PHI.

81. Defendants have not provided credit monitoring and identity theft protection to Plaintiffs and Class members.

82. Additionally, Defendants have not taken the actions necessary and recommended by the FBI, CISA, NSA and other experts detailed above to prevent an attack by criminals, leaving Plaintiffs and Class members vulnerable to subsequent breaches of their PHI.

83. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failures to implement or maintain adequate data security measures for the PHI of Plaintiffs and Class members.

Plaintiffs' Experiences

84. Plaintiffs received healthcare from Mercy Health. As a condition of obtaining treatment, Plaintiffs provided PHI to Mercy Health with the reasonable expectation that Defendants would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use their PHI for legitimate business purposes as laid out in the notice of privacy practices.

85. Defendants expressly and impliedly promised to safeguard Plaintiffs' PHI. Defendants assumed obligations to Plaintiffs, and Plaintiffs relied on Defendants to safeguard their PHI and only to utilize it for legitimate business purposes. Defendants, however, did not take proper care of Plaintiffs' PHI, leading to exposure as a direct result of Defendants' inadequate security measures and negligent data security and retention policies. Had Plaintiffs known that their PHI would be insufficiently protected from known cyberthreats, Plaintiffs would not have disclosed the information to Defendants and would not have paid as much as they did for the healthcare services they bargained to receive—of which confidentiality was a material term.

86. After November 8, 2023, Plaintiff Bishop received notice from Defendants that his PHI had been improperly accessed and obtained by unauthorized third parties. *See* Exhibit 2.

87. Plaintiff Metzger received his letter notifying him of the Data Breach on November 28, 2023. *See* Exhibit 3.

88. As a result of the Data Breach, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing financial, healthcare, and other accounts for any indications of actual or attempted identity theft or fraud. Plaintiffs have spent time dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work or recreation.

89. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their PHI, which they reasonably believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using the PHI for purposes of identity theft and fraud. Plaintiffs are very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

90. Plaintiffs suffered actual injury from having their PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their PHI, a form of property that Defendants obtained from Plaintiffs; (b) violation of their privacy rights; (c) loss of the benefit bargained for data security protections; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

91. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiffs and Class members will always have to protect against the possibility that incorrect information was entered in their medical records as a result of undetected identity fraud, which may result in substandard care and negative health consequences. They also face the risk of embarrassment and loss of privacy should their PHI be publicized or disseminated to third parties.

CLASS ACTION ALLEGATIONS

94. Plaintiffs, individually and on behalf of others similarly situated, seek to certify the following class and subclasses of similarly situated persons under Rule 23 of the Federal Rules of Civil Procedure:

> **Nationwide Class.** All persons in the United States whose PHI was accessed by criminals in the Data Breach.
>
> **Ohio Subclass.** All Ohio residents whose PHI was accessed by criminals in the Data Breach.
>
> **Mercy Health Subclass.** All persons who received treatment from Mercy Health whose PHI was accessed by criminals in the Data Breach.

95. Excluded from the Nationwide Class, Ohio Subclass, and Mercy Health Subclass (the "Classes") are Defendants' officers and directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their immediate families and members of their staff.

96. Plaintiffs reserve the right to amend or modify the Class definitions and/or create additional subclasses as this case progresses.

97. **Numerosity.** The members of the Classes are so numerous that joinder of all of them is impracticable. The Class consists of approximately 9 million individuals based on Defendants' reports to the HHS data breach portal.

98. **Commonality.** There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' PHI;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class members to safeguard their PHI;

f. Whether Defendants breached their duties to Class members to safeguard their PHI;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' acts, inactions, and practices complained of herein breached implied contracts with Plaintiffs and Class members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class members; and

m. Whether Plaintiffs and Class members are entitled to damages, punitive damages, treble damages, and/or injunctive or other equitable relief.

99. **Typicality.** Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class member, was compromised in the Data Breach.

100. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' counsel is competent and experienced in litigating class actions.

101. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiffs and Class members, in that all of Plaintiffs' and Class members' PHI was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

102. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

103. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(on behalf of Plaintiffs and the Classes)

104. Plaintiffs reallege paragraphs 1–103 as if fully set forth herein.

105. As a condition of obtaining treatment, Plaintiffs and Class members provided Defendants with their PHI.

106. Plaintiffs and Class members entrusted their PHI to Defendants with the understanding and relying upon Defendants to exercise reasonable care in the protection of their PHI.

107. Defendants had a duty to take reasonable measures to protect the PHI of Plaintiffs and Class members from unauthorized disclosure to third parties. This duty is inherent in the nature of the exchange of highly sensitive personal information in connection with the patient-physician relationship.

108. Defendants have full knowledge of the sensitivity of the PHI and the types of harm that Plaintiffs and Class members could and would suffer if the PHI were wrongfully disclosed in a Data Breach.

109. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, using, and retaining of the PHI of Plaintiffs and Class members, without adequate data security, involved an unreasonable risk of harm to Plaintiffs and Class members.

110. Defendants had duties to exercise reasonable care in safeguarding, securing, retaining, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. These duties include, among other things, designing, configuring, maintaining, and testing security protocols to ensure that the PHI of Plaintiffs and Class members in Defendants' possession was adequately secured and protected.

111. Defendants had a duty to exercise appropriate practices to remove PHI that was no longer required.

112. Defendants had a duty to encrypt the PHI they stored and maintained.

113. Defendants had a duty to segregate the PHI from other portions of their networks accessible from the outside.

114. Defendants had a duty to properly train employees and vendors to recognize phishing attempts and other common data security risks.

115. Defendants had a duty to implement and maintain procedures to detect and prevent the improper access, exfiltration, and misuse of PHI to their systems and their vendors' systems.

116. Defendants' duty to use reasonable security measures arose as a result of the relationship that existed between Defendants and Plaintiffs and Class members. Plaintiffs and Class members entrusted Defendants with their PHI and relied upon Defendants to implement adequate data security and reasonable data retention policies.

117. Defendants were subject to an independent duty untethered to any contract between Defendants and Plaintiffs or Class members.

118. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class members was reasonably foreseeable, particularly in light of Defendants' inadequate

security practices, the detailed warnings published by governmental agencies, and news reports of other data breaches.

119. Plaintiffs and Class members were the foreseeable and probable victims of Defendants' inadequate and unreasonable data security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PHI, the critical importance of providing adequate security of that PHI, the necessity for encrypting PHI, and the harm that can arise from retaining PHI following the expiration of any legitimate business purpose.

120. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and Class members. Defendants solicited, collected, generated, digitized, and aggregated and organized Plaintiffs' and Class members' PHI, failed to encrypt the PHI, failed to maintain proper oversight over the security of their systems or the systems of their vendors, failed to implement other reasonable industry standard measures to safeguard PHI, and failed to implement retention policies that delete PHI.

121. Plaintiffs and Class members had no ability to protect their PHI that was in, and remains in, Defendants' possession, and no sign that Defendants were failing and refusing to implement and maintain reasonable data security practices over their PHI until they received their notification letters.

122. Defendants placed Plaintiffs' and Class members' PHI in a risky location that was attractive to cybercriminals, and Defendants were the only ones able to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

123. Defendants had and continue to have a duty to adequately disclose that the PHI might have been compromised, how it was compromised, and precisely the types of data that

were compromised and when. Such notice is necessary to allow Plaintiffs and the Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI.

124. Defendants had a duty to employ proper procedures to prevent the unauthorized disclosure and unauthorized sharing of the PHI to criminals.

125. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to implement and maintain industry-standard protocols and to exercise reasonable care in protecting and safeguarding the PHI of Plaintiffs and Class members.

126. Defendants improperly and inadequately safeguarded the PHI of Plaintiffs and Class members in violation of standard industry rules, regulations, and practices at the time of the Data Breach.

127. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized downloading and dissemination of PHI.

128. Defendants breached their duty to remove PHI that was no longer needed.

129. Defendants breached their duties to encrypt PHI and to segregate it from other portions of their networks.

130. Defendants breached their duties to adequately train employees and vendors to recognize and avoid phishing attempts and other basic cybersecurity risks.

131. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and Class members the existence and scope of the Data Breach.

132. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class members, the PHI of Plaintiffs and Class members would not have been compromised.

133. There is a close causal connection between Defendants' failure to implement security measures to protect the PHI of Plaintiffs and Class members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class members. The PHI of Plaintiffs and Class members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

134. As a direct and proximate result of Defendants' numerous negligent acts and omissions, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

135. Plaintiffs and Class members have and will continue to closely monitor their financial and medical records to guard against future identity theft and fraud. Such mitigation efforts included, and will include into the future, protective steps: *e.g.*, reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

136. As a direct and proximate result of Defendants' numerous negligent acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of

identity theft; (d) financial costs incurred due to actual identity theft; (e) the cost of future identity theft monitoring; (f) loss of time incurred due to actual identity theft; (g) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (h) and diminution of value of their PHI.

137. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI. Plaintiffs and Class members are, therefore, also seeking injunctive relief for the continued risk to their PHI from future breaches, so long as Defendants fail to undertake appropriate and adequate measures to safeguard the PHI.

138. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT II
Negligence *per se*
(on behalf of Plaintiffs and the Classes)

139. Plaintiffs reallege paragraphs 1–138 as if fully set forth herein.

140. Defendants, as health care providers who transmit health information in electronic form, are covered entities as defined by 45 C.F.R. § 160.103.

141. Defendants violated HIPAA regulations, including by:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

g) Failing to ensure compliance with HIPAA security standard rules by their workforce, in violation of 45 C.F.R. section 164.306(a)(4);

h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

i) Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

142. Defendants also violated the duties applicable to them under the Federal Trade Commission Act (15 U.S.C. § 45, et seq.) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

143. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One*, 488 F. Supp. 3d at 407.

144. Plaintiffs' and Class members' PHI was and is nonpublic personal information and customer information.

145. Plaintiffs and Class members are in the group of persons that HIPAA and the FTC Act were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendants' violations of HIPAA and the FTC Act were the types of harm the statutes and regulations are designed to prevent.

146. As a direct and proximate result of Defendants' numerous negligent acts and omissions, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

147. As a direct and proximate result of the conduct of Defendants that violated HIPAA and the FTC Act, Plaintiffs and Class members have suffered and will continue to suffer the foreseeable economic and non-economic harms as described herein.

148. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT III
Negligent Misrepresentation
Against Mercy Health
(on Behalf of Plaintiffs and the Mercy Health Subclass)

149. Plaintiffs reallege paragraphs 1–148 as if fully set forth herein.

150. Defendant supplied false information for the guidance of others in the course of its business. As alleged above, Defendant falsely represented that its superior data security practices would protect Plaintiffs and Class members from the Data Breach, when in actuality, Defendant employed deficient and unreasonable data security practices.

151. Defendant's representations were false and Defendant failed to exercise reasonable care in obtaining or communicating the information. Defendant's data security practices were unreasonable and deficient by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiffs' and Class members' PHI;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiffs' and other Class members' PHI;

d. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiffs' and other Class members' PHI;

e. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiffs' and other Class members' PHI reasonably and appropriately in order to repel or limit the Data Breach;

f. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PHI to ensure the PHI was being stored and maintained for legitimate and useful purposes;

g. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendant's sensitive

business information would not expose and cause disclosure and unauthorized acquisition of Plaintiffs' and other Class members' PHI;

h. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

i. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

j. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiffs and other Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PHI, and details regarding the disposition of Plaintiffs' and other Class members' PHI at all times during the Data Breach.

152. Plaintiffs and Class members justifiably relied on Defendant's false information and were induced to obtain Defendant's products and services in reliance thereon.

153. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the data breach, including the instructions in the Data Breach notice letter; (e) the cost of future monitoring for identity theft, including medical identity theft; (f) loss of time

and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PHI.

154. As a direct and proximate result of Defendant's negligent misrepresentation, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT IV
Negligent Entrustment
Against Mercy Health
(on Behalf of Plaintiffs and the Mercy Health Subclass)

155. Plaintiffs reallege paragraphs 1–154 as if fully set forth herein.

156. Mercy Health owed a duty to Plaintiffs and the Class to adequately safeguard the private information that it required its customers to provide. Part and parcel of this duty was the duty to only entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

157. Mercy Health breached this duty by entrusting PJ&A with the private information of its customers when, as described throughout the Complaint, it knew or should have known that PJ&A utilized software that was incompetent at preventing such unauthorized disclosure.

158. As a direct and proximate result of Defendant's failure to exercise reasonable care in selecting with whom to entrust its customers' private information, the personal data of Defendant's customers was accessed by ill-intentioned criminals who could and will use the information to commit identity theft or financial fraud. Plaintiffs and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and misuse of their personal data.

159. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the

following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the data breach, including the instructions in the Data Breach notice letter; (e) the cost of future monitoring for identity theft, including medical identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PHI.

160. As a direct and proximate result of Defendant's negligent entrustment, Plaintiffs and Class members are entitled to recover actual and punitive damages.

COUNT V
Breach of Implied Contract
Against Mercy Health
(on behalf of Plaintiffs and the Mercy Health Subclass)

161. Plaintiffs reallege paragraphs 1–160 as if fully set forth herein.

162. Mercy Health required Plaintiffs and Class members to provide their PHI as a condition of receiving treatment. In so doing, Plaintiffs and Class members entered into implied contracts with Mercy Health wherein Mercy Health agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their PHI had been breached and compromised or stolen.

163. Mercy Health further entered into an implied contract with Plaintiffs and the Class members to honor its representations and assurances regarding protecting their PHI.

164. Plaintiffs and Class members fully performed their obligations under implied contracts with Mercy Health.

165. Mercy Health, through its own actions and omissions and through those of its agent PJ&A, breached the implied contracts it made with Plaintiffs and Class members by (i)

failing to implement technical, administrative, and physical security measures to protect the PHI from unauthorized access or disclosure, despite such measures being readily available, (ii) failing to limit access to the PHI to those with legitimate reasons to access it, (iii) failing to store the PHI only on servers kept in a secure, restricted area, and (iv) otherwise failing to safeguard the PHI.

166. As a direct and proximate result of Mercy Health's breach of its implied contract, Plaintiffs and Class members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

167. As a direct and proximate result of Mercy Health's breach of implied contract, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) financial costs incurred due to actual identity theft; (d) the cost of future identity theft monitoring; (e) loss of time incurred due to actual identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; (g) failure to receive the benefit of their bargained for data protection for which Plaintiffs and Class members paid a premium to CCH; and (h) diminution of value of their PHI.

168. As a direct and proximate result of the above-described breaches of implied contract, Plaintiffs and Class members are entitled to recover actual, consequential, and nominal damages.

COUNT VI
Invasion of Privacy – Intrusion Upon Seclusion
(on Behalf of Plaintiffs and the Classes)

169. Plaintiffs reallege paragraphs 1–168 as if fully set forth herein.

170. Plaintiffs and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

171. Defendants intruded upon that seclusion by allowing the unauthorized access to the Plaintiffs and Class members' PII without Plaintiffs' and Class members' consent, knowledge, authorization, notice, or privilege by negligently maintaining the confidentiality of Plaintiffs' and Class members' information as set out above.

172. Defendants' breach of confidentiality resulted in insecure systems allowing harmful disclosure of the information to criminals and criminal data markets.

173. The intrusion was offensive and objectionable to Plaintiffs, the Class members and to a reasonable person or ordinary sensibilities in that Plaintiffs' and Class members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

174. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class members provided and disclosed their PII to Defendants privately with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class members were reasonable to believe that such information would be kept private and would not be disclosed without consent. Plaintiffs and the Class members were further reasonable to believe that the PII would be reasonably protected against third-party criminal extraction through foreseeable hacking activity.

175. This improper disclosure increased the risk that the personal data was delivered to criminal data markets thereby increasing the risk of identity theft to Plaintiffs and the Class members.

176. The harm included the erosion of the essential confidential relationship between the patient and the healthcare provider.

177. As a direct and proximate result of Defendants' unauthorized disclosure, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the data breach, including the instructions in the Data Breach notice letter; (e) the cost of future monitoring for identity theft, including medical identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PHI.

COUNT VII
Unjust Enrichment
(on behalf of Plaintiffs and the Classes)

178. Plaintiffs reallege paragraphs 1–177 as if fully set forth herein.

179. This claim is brought in the alternative.

180. Defendants benefited from receiving Plaintiffs' and Class members' PHI by their ability to retain and use that information for their own benefit.

181. Defendants also understood and appreciated that Plaintiffs' and Class members' PHI was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

182. Plaintiffs and Class members conferred a benefit upon Defendants by paying for services, and in connection therewith, by providing their PHI to Defendants with the understanding that Defendants would implement and maintain reasonable data privacy and security practices and procedures. Plaintiffs and Class members should have received adequate protection and data security for such PHI held by Defendants.

183. Defendants knew Plaintiffs and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and appreciated the benefits.

184. Defendants failed to provide reasonable security, safeguards, and protections to the PHI of Plaintiffs and Class members.

185. Defendants should not be permitted to retain money rightfully belonging to Plaintiffs and Class members, because Defendants failed to implement appropriate data security measures and caused the Data Breach.

186. Defendants accepted and wrongfully retained these benefits to the detriment of Plaintiffs and Class members.

187. Defendants' enrichment at the expense of Plaintiffs and Class members is and was unjust.

188. As a result of Defendants' wrongful conduct, as alleged above, Plaintiffs and Class members seek restitution of their money paid to Defendants, and disgorgement of all profits, benefits, imposition of a constructive trust, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

COUNT VIII
Disclosure of Non-Public Information
pursuant to *Biddle v. Warren Gen. Hosp.,* 86 Ohio St. 3d 395 (1999)
Against Mercy Health
(on Behalf of Plaintiffs and the Mercy Health Subclass)

189. Plaintiffs reallege paragraphs 1–188 as if fully set forth herein.

190. In Ohio, medical providers have an obligation to their patients to keep non-public medical information completely confidential.

191. Disclosure of medical information by a medical provider in Ohio without consent results in civil liability.

192. Plaintiffs and Class members are each patients of the Defendant.

193. Plaintiffs and each Class member had a reasonable expectation of privacy in their private information.

194. Contrary to its legal obligations as medical providers, and its implied contract to maintain the confidentiality of its patients, Defendant disclosed the information without Plaintiffs' or the Class members' consent.

195. In addition, by and through its negligence, and/or in combination with PJ&A's negligence, Plaintiffs and Class members' private information was disclosed to a third-party criminal enterprise.

196. This improper disclosure increased the risk that the personal data was delivered to criminal data markets thereby increasing the risk of identity theft to Plaintiffs and the Class members.

197. The harm included the erosion of the essential confidential relationship between the patient and the healthcare provider.

198. As a direct and proximate result of Defendant's unauthorized disclosure, Plaintiffs and Class members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the data breach, including the instructions in the Data Breach notice letter; (e) the cost of future monitoring for identity theft, including medical identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PHI.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, pray for judgment against Defendants and in Plaintiffs' favor, as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PHI compromised during the Data Breach;

d) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

e) For an award of punitive damages, as allowable by law;

f) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

g) Pre- and post-judgment interest on any amounts awarded; and,

h) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 22, 2023

Respectfully Submitted,

/s/ *Marc E. Dann*
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
**Pro Hac Vice Application Anticipated*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com

Attorneys for Plaintiffs and the proposed Classes